МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет информатики и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью

Кафедра Информационных технологий и безопасности компьютерных систем
Факультета Информатики и информационных технологий

Образовательная программа

10.03.01 -Информационная безопасность

Профиль подготовки Безопасность компьютерных систем

Уровень высшего образования
Бакалавриат

Форма обучения
Очная, очно-заочная

Статус дисциплины:
входит в обязательную часть ОПОП

Махачкала, 2021

Рабочая программа дисциплины «Основы управления информационной безопасностью» составлена в 2021 году в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01_Информационная безопасность от «7» ноября 2020г. №1427.

Разработчик: Гаджиев Амир Маликович кан. физ.мат.н., доцент кафедры информационных технологий и безопасности компьютерных систем

Рабочая программа дисциплины одобрена:
на заседании кафедры ИТиБКС от « 28 » 06__2021 г., протокол № 11

Зав. Кафедрой_____ Ахмедова З.Х.

(подпись)

на заседании Методической комиссии факультета ИиИТ

от «*29*», 06_2021 протокол № 11

Председатель_____Бакмаев А.Ш.

(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «____» _____20__г.

Начальник УМУ _____Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Основы управления информационной безопасностью» является базовой дисциплиной образовательной программы бакалавриата по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется на факультете Информатики и ИТ кафедрой Информационных технологий и безопасности компьютерных систем.

Содержание дисциплины охватывает круг вопросов, связанных с изучением современных подходов, методов и методик создания системы управления информационной безопасностью предприятий и организаций, приобретением практических навыков по разработке надежной системы управления информационной безопасности.

Дисциплина нацелена на формирование следующих компетенций выпускника: универсальных - УК-4; общепрофессиональных - ОПК-1, ОПК – 1.1.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме *контрольной работы или тестирования* и промежуточный контроль в форме зачета.

Объем дисциплины 5 зачетных единиц, в том числе в академических часах по видам учебных занятий

Очная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	контроль		
7	180	52	34	0	18		0	128	экзамен

Очно-заочная форма обучения

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:								
	всего	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
		всего	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР			
7	180	86	16	0	16			0	148	экзамен

1. Цели освоения дисциплины

Целями изучения дисциплины «Основы управления информационной безопасностью» является:

формирование навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ;

создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ;

развитие способностей по использованию существующей системы управления информационной безопасности.

2. Место дисциплины в структуре ОПОП бакалавлиата

Дисциплина «Основы управления информационной безопасностью» является базовой дисциплиной образовательной программы бакалавриата по направлению 10.03.01 «Информационная безопасность».

Изучение дисциплины базируется на знаниях, полученных студентами при изучении дисциплин «Основы управленческой деятельности», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Программно- аппаратные средства защиты информации», «Защита и обработка конфиденциальных документов». Изучение дисциплины позволяет овладеть как теоретической базой, так и конкретными практическими навыками по организации и управлению информационной безопасностью.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Дисциплина «Основы управления информационной безопасностью» обеспечивает инструментарий формирования следующих ОПК компетенций:

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции	Результаты обучения
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и	ИД1.УК-2.1.Знает необходимые для осуществления профессиональной деятельности правовые нормы	Знает необходимые для осуществления профессиональной деятельности правовые нормы
	ИД2.УК-2.2.Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной	Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов

ограничений	деятельности	
	ИД3.УК-2.3.Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.	Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД1.ОПК-1.1.Знать. организационно – правовую основу информационной безопасности и средства ее обеспечения	Знает основные правовые и организационные положения, перечень мероприятий по поддержанию информационной безопасности на должном уровне
	ИД2.ОПК-1.2.Уметь . использовать права и обязанности граждан государства в рамках правового пространства для обеспечения защиты информации	Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.
	ИД3.ОПК-1.3. Владеть навыками оперативного отслеживания нарушений прав пользователей телекоммуникационной системы и анализа информационных процессов в этих системах, способами моделирования информационных процессов в телекоммуникациях	Имеет навыки теоретического и экспериментального исследования объектов профессиональной деятельности.
ОПК-1.1 . Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах;	ИД1.ПК-1.1. Знает современные инструментальные средства, методы программного обеспечения управления доступом в ком. системах	Знает: современные инструментальные средства программного обеспечения
	ИД2.ПК-1.2. Умеет анализировать и выбирать инструментальные средства программного обеспечения для управления доступом	Умеет: анализировать и выбирать инструментальные средства программного обеспечения
	ИД3.ПК-1.3. Владеет навыками использования методов управления политики безопасности и инструментальных средств исследования программного обеспечения управления доступом	Владеет: навыками использования методов управления политики безопасностии инструментальных средств исследования программного обеспечения

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 5 зачетных единиц, 180 академических часов.

4.2. Структура дисциплины. _____

Очная форма обучения

№ п/п	Разделы и темы дисциплины	Семестр	Очная форма обучения	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практичес кие	Лаборат.за	СРС		
Модуль 1. Базовые вопросы управления информационной безопасностью									
1.	Основные понятия информационной безопасности	7	1	2				2	
2.	Угрозы информационной безопасности в информационных системах	7	2	2	2			4	
3.	Стандарты управления информационной безопасностью	7	3	1				6	
4.	Стандарты управления информационной безопасностью	7	4	1				6	
5.	Создание СУИБ на предприятии	7	5	2	2			6	
	Итого по модулю 1:		6	8	4			24	Тестирование по мод
Модуль 2 Методы оценки информационных рисков И							НС		
6.	Методика оценки рисков информационной безопасности компании	7	7	2	2			4	
7.	Метод оценки рисков на основе модели информационных потоков	7	8	2				6	
8.	Методики и технологии управления рисками	7	9	2	2			6	
9.	Разработка корпоративной методики анализа рисков	7	10	2	2			6	
	Итого по модулю 2:	7	11	8	6			22	Тестирование по мод
Модуль 3 Современные методы и средства обеспечения ИБ									

10.	Современные методы и средства анализа и управление рисками информационных систем компаний	7	12	2				6	
11.	Правовое обеспечение ИБ	7	12	2				6	
12.	Организационные меры обеспечения безопасности компьютерных информационных систем	7	13	2	2			6	
13.	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом "	7	14	2	2			6	
	Итого по модулю3:		15	8	4			24	Тестирование по мод
Модуль 4 **Основы криптографии и защита информации в ИС**									
10.	Основы криптографии.	7	16	2	2			6	
11.	Средства защиты информации в автоматизированных системах	7		2				4	
12.	Обеспечение высокой доступности, **т**уннелирование и управление	7	17	2				6	
1□.	Методология построения защищенных автоматизированных информационных систем	7	18	4	2			4	
	Итого по модулю3:			10	6			20	Тестирование по мод
Модуль 5 Подготовка к экзамену									
	Итого по модулю3:							36	Тестиро□ание по мод
Итого по курсу		180		34	18			128	экзамен

Очно-заочная форма обучения

№ п/п	Разделы и темы дисциплины	Семестр	Очная форма	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)	Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной

				Лекции	Практичес кие	Лаборат.за	СРС		аттестации *(по семестрам)*
Модуль 1. Базовые вопросы управления информационной безопасностью									
1.	Основные понятия информационной безопасности	7	1	1				2	
2.	Угрозы информационной безопасности в информационных системах	7	2	1	2			4	
3.	Стандарты управления информационной безопасностью	7	3	1				6	
4.	Стандарты управления информационной безопасностью	7	4	1				6	
5.	Создание СУИБ на предприятии	7	5		2			6	
	Итого по модулю 1:		6	4	4			28	Тестирование по мод
Модуль 2 Методы оценки информационных рисков И							НС		
6.	Методика оценки рисков информационной безопасности компании	7	7	0	2			4	
7.	Метод оценки рисков на основе модели информационных потоков	7	8	2				6	
8.	Методики и технологии управления рисками	7	9	2	0			6	
9.	Разработка корпоративной методики анализа рисков	7	10	0	2			6	
	Итого по модулю 2:	7	11	4	4			26	Тестирование по мод
Модуль 3 Современные методы и средства обеспечения ИБ									
10.	Современные методы и средства анализа и управление рисками информационных систем компаний	7	12	1				6	
11.	Правовое обеспечение ИБ	7	12	1				6	
12.	Организационные меры обеспечения безопасности компьютерных информационных систем	7	13	1	2			6	
13.	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом "	7	14	1	2			6	

	Итого по модулю3:		15	4	4			28	Тестирование по мод
Модуль 4 **Основы криптографии и защита информации в ИС**									
□0.	Основы криптографии.	7	16	1	2			6	
11.	Средства защиты информации в автоматизированных системах	7		1				4	
12.	Обеспечение высокой доступности, туннелирование и управление	7	17	1				6	
13.	Методология построения защищенных автоматизированных информационных систем	7	18	1	2			4	
	Итого по модулю3:			4	4			20	Тестирование по мод
Модуль 5 Подготовка к экзамену									
	Итого по модулю3:							36	Тестирование по мод
Итого по курсу		180		16	16			148	экзамен

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине

Модуль 1. Базовые вопросы управления информационной безопасностью

Тема 1: "Основные понятия информационной безопасности"

Вопросы:

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Управление информационной безопасностью.
4. Важность и сложность проблемы информационной безопасности

Тема 2: "Угрозы информационной безопасности в информационных системах"

Вопросы:

1. Основные определения и критерии классификации угроз.
2. Основные угрозы доступности.
3. Основные угрозы целостности.
4. Основные угрозы конфиденциальности.
5. Вредительские программы

Тема 3: «Оценочные стандарты в информационной безопасности»
Вопросы:

1. Роль стандартов ИБ.
2. «Оранжевая книга» как оценочный стандарт.
3. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Тема 4: «Стандарты управления информационной безопасностью»
Вопросы:

1. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.
2. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".
3. Сертификация СУИБ на соответствие ISO 27001

Тема 5: "Создание СУИБ на предприятии"
Вопросы:

1. Этапы разработки и внедрения системы управления ИБ.
2. Содержание этапов разработки и внедрения системы управления ИБ.

Модуль 2 Методы оценки информационных рисков ИС

Тема 6: "Методика оценки рисков информационной безопасности компании"
Вопросы:

1. Управление рисками. Основные понятия.
2. Метод оценки рисков на основе модели угроз и уязвимостей

Тема 7: «Метод оценки рисков на основе модели информационных потоков»
Вопросы:

1. Расчет рисков по угрозе конфиденциальность
2. Расчет рисков по угрозе целостность

Тема 8: Методики и технологии управления рисками
Вопросы:

1. Качественные методики управления рисками.
2. Методики COBRA и RA Software Tool.
3. Количественные методики управления рисками.
4. Метод CRAMM.

Тема 9: "Разработка корпоративной методики анализа рисков"
Вопросы:

1. Постановка задачи

2. Методы оценивания информационных рисков
3. Табличные методы оценки рисков
4. Методика анализа рисков Microsoft

Модуль 3 Современные методы и средства обеспечения ИБ

Тема 10: " Современные методы и средства анализа и управление рисками информационных систем компаний"

Вопросы:

1. Обоснование необходимости инвестиций в информационную безопасность компании.
2. Методика FRAP (фреп).
3. Методика OCTAVE (октэйв)
4. Методика Risk Watch (риск вэтч).

Тема 11: «Правовые меры обеспечения безопасности компьютерных информационных систем»

Вопросы:

1. Обзор российского законодательства в области информационной безопасности
2. Закон "Об информации, информатизации и защите информации"
3. Другие законы и нормативные акты
4. О текущем состоянии российского законодательства в области информационной безопасности
5. Обзор зарубежного законодательства в области информационной безопасности

Тема 12: «Организационные меры обеспечения безопасности компьютерных информационных систем»

Вопросы

1. Общие положения организационной защиты.
2. Особенности организационной защиты компьютерных информационных систем и сетей.
3. Управление информационной безопасности предприятия.

Тема 13: «Программно-технические меры обеспечения безопасности компьютерных информационных систем»

Вопросы:

1. Основные программно-технические меры.
2. Идентификация и аутентификация.
3. Управление доступом.

4.3 .2. ***Содержание лабораторно-практических занятий по дисциплине.***

Тема 1. Введение. Базовые вопросы управления ИБ. Процессный подход

Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.).

Тема 2. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ

- Разработка и управление политикой ИБ информационной системы

Тема 3.Рискология ИБ

- Анализ модели угроз ИБ и уязвимостей
- Анализ модели информационных потоков

Тема 4.Основные процессы СУИБ. Обязательная документация СУИБ

-Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»).

- Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса».

-Процесс «Анализ со стороны высшего руководства». -Процесс «Обучение и обеспечение осведомленности».

Тема 5.Эксплуатация и независимый аудит СУИБ

Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации

Тема 6.Внедрениеразработанных процессов. Документ «Положение о применимости»

Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

Тема 7. Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса»

Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

Тема 8.Обеспечение соответствия требованиям законодательства РФ

Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

№ п/п	№ темы дисцип-лины	Тематика практических занятий (семинаров)	Технология проведения	Трудоём-кость в часах
1	**1-5**	Анализ и оценка управленческих и экономических показателей системы управления обеспечением информационной безопасности бизнеса.	Теоретическая справка с кратким изложением основных понятий. Проведение ситуационных моделей происходит в интерактивной форме для отработки навыков управления информационной безопасностью Выступления студентов с докладами и презентациями. Аудиторные самостоятельные работы для качественной оценки пройденного материала (15-20 мин.).	6
2	**6-9**	Управление жизненным циклом информационных активов.		6
3	**10-13**	Анализ влияния информационного риска на деятельность организации.		6
		ИТОГО		18

5. Образовательные технологии

Основными образовательными технологиями проведения курса «Основы управления информационной безопасностью» являются:

- Лекции, сопровождаемые компьютерными презентациями;
- практические занятия, в рамках которых составляются и тестируются программы, иллюстрирующие теоретический материал лекций;
- самостоятельная работа студентов, включающая усвоение теоретического материала, поиск дополнительного материала и эффективных способов выполнения заданий, оформление и подготовка к практическому занятию, подготовка к текущему контролю знаний и к итоговому экзамену;
- разработанные индивидуальные задания для самостоятельной работы;

• рейтинговая технология контроля учебной деятельности студентов для обеспечения их ритмичной работы в течение семестра

• консультирование студентов по вопросам учебного материала и выполнения курсового

заданий.

6. Учебно-методическое обеспечение самостоятельной работы студентов

При изучении дисциплины «Основы управления информационной безопасностью» обязательными являются следующие виды самостоятельной работы:

- разбор теоретического материала по учебным пособиям и конспектам лекций;

- самостоятельное изучение указанных теоретических вопросов; подготовка к проведению ситуационных моделей в интерактивной форме;

Очная форма

№	Модули и темы	Виды СРС		Объем часов
		обязательные	дополнительные	
Модуль 1				
1.1	Введение. Базовые вопросы управления ИБ. Процессный подход.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой	8
1.2	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу.	Работа с учебной литературой	8
1.3.	Рискология ИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой,	8
	Всего по модулю 1:			**24**
Модуль 2				
2.1.	Основные процессы СУИБ. Обязательная документация СУИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к	Работа с учебной литературой	12

		докладу.		
2.2	Эксплуатация и независимый аудит СУИБ.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу, подготовка к ответу на коллоквиуме.	Работа с учебной литературой,	10
	Всего по модулю 2:			**22**
Модуль 3				
3.1	Внедрение разработанных процессов. Документ «Положение о применимости»	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой,	8
3.2	Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведения бизнеса»	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой, выполнение расчетной работы на компьютере	8
3.3	Обеспечение соответствия требованиям законодательства РФ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой.	8
	Всего по модулю 3:			**24**
Модуль 4				
3.1	Основы криптографии.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой,	8
3.2	Средства защиты информации в автоматизированных системах	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой, выполнение расчетной работы на компьютере	6
3.3	Обеспечение высокой доступности, туннелирование и управление	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к	Работа с учебной литературой,.	6

		ответу на коллоквиуме.		
	Всего по модулю 4:			**20**
	ИТОГО:			**128**

Очно - заочная форма

№	**Модули и темы**	**Виды СРС**		**Объем часов**
		обязательные	**дополнительные**	
Модуль 1				
1.1	Введение. Базовые вопросы управления ИБ. Процессный подход.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой	8
1.2	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу.	Работа с учебной литературой	8
1.3.	Рискология ИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой,	8
	Всего по модулю 1:			**24**
Модуль 2				
2.1.	Основные процессы СУИБ. Обязательная документация СУИБ	Конспектирование материала на лекционных занятиях. Подготовка к ответу на семинаре и к докладу.	Работа с учебной литературой	20
2.2	Эксплуатация и независимый аудит СУИБ.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу, подготовка к ответу на коллоквиуме.	Работа с учебной литературой,	10
	Всего по модулю 2:			**30**

Модуль 3				
3.1	Внедрение разработанных процессов. Документ «Положение о применимости»	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой,	8
3.2	Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведения бизнеса»	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой, выполнение расчетной работы на компьютере	8
3.3	Обеспечение соответствия требованиям законодательства РФ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой.	10
	Всего по модулю 3:			**26**
Модуль 4				
3.1	Основы криптографии.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой,	10
3.2	Средства защиты информации в автоматизированных системах	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой, выполнение расчетной работы на компьютере	10
3.3	Обеспечение высокой доступности, **т**уннелирование и управление	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой,.	10
	Всего по модулю 4:			**30**
	ИТОГО:			**148**

Контроль результатов освоения дисциплины

Текущий контроль успеваемости осуществляется путем оценки результатов выполнения заданий лабораторных, самостоятельной работ, посещения лекций.

Промежуточная аттестация осуществляется в форме экзамена, который выставляется по результатам проверки выполнения тестов и заданий.

Оценочные средства результатов освоения дисциплины, критерии оценки выполнения заданий представлены в разделе «Фонды оценочных средств для проведения промежуточной аттестации» и фонде оценочных средств образовательной программы.

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.1. Типовые контрольные задания или иные материалы

1. Законодательство в области информационной безопасности
2. Криптографические методы и средства защиты информации в компьютерных системах и сетях
3. Политика и модели безопасности
4. Безопасность сетевых операционных систем
5. Безопасность локальных и глобальных сетевых технологий
6. Радиоэлектронные системы и устройства защиты информации
7. Комплексная защита информации в компьютерных системах и сетях Актуальность проблем информационной безопасности в современном мире.
8. Задачи и методы обеспечения информационной безопасности в сфере внешней и внутренней политики России.
9. Информация - наиболее ценный ресурс современного общества.
10. Проблемы информационных войн на современном этапе.
11. Государственная информационная политика РФ.
12. Государственная система правового обеспечения защиты информации в РФ.
13. Государственное регулирование использования криптографических средств.
14. Государственное регулирование использования электронной цифровой подписи.
15. Информационная безопасность в государственной информационной политике РФ.
16. Информациякак объект юридической защиты.
17. Информационное право на современном этапе развития общества.
18. Задачи и принципы организации службы информационной безопасности предприятий.
19. Зарубежное законодательство в области информационной безопасности.
20. Зарубежные стандарты в области информационной безопасности.
21. Информационная безопасность беспроводных сетей.
22. Информационная безопасность компьютерных сетей.
23. Современное информационное оружие и его классификация.
24. Информациякак наиболее ценный ресурс современного общества.

25. Категорииинформации по режиму ограничения доступа и использования.
26.Лицензирование, сертификация и аттестация объектов информатизации и защиты информации.
27. Использованиекриптографических и стеганографических методов в информационном обмене.
28.Международные стандарты информационного обмена.
29.Обеспечение информационной безопасности в Internet.
30.Основные положения Доктрины информационной безопасности.
31.Отечественные стандарты в области информационной безопасности.
32. Оценка безопасности информационных технологий.
33.Организационная структура государственной системы обеспечения информационной безопасности РФ.
34. Базовые источники системы информационной безопасности.
35. Правонарушения и ответственность в области эксплуатации информационных систем и информационной безопасности.
36. Правовая основа системы информационной безопасности.
37. Нормативно-правовое обеспечение в сфере связи и коммуникаций.
38. Корпоративная политика информационной безопасности.
39. Проблемы информационной безопасности в национальном и международном аспектах.
40. Проблемы информационной безопасности в области государственного и муниципального управления.
41. Программно-технический уровень информационной безопасности.
42. Современное состояние нормативно-правовой базы информационной безопасности.
43. Система подготовки кадров в области информационной безопасности в РФ.
44. Угрозы безопасности информации и информационные атаки.
45. Угрозы информационной безопасности в компьютерных сетях.
46. Управление информационными рисками.
47. Электронная цифровая подпись - правовой и технический

Типовые контрольные задания

1. Под угрозой безопасности информации в компьютерной системе (КС) понимают:
2. Уязвимость информации — это: _____
3. Атакой на КС называют: _____
4. Искусственные угрозы исходя из их мотивов разделяются на:
5. непреднамеренным угрозам относятся: _____
6. К умышленным угрозам относятся: _____
7. Косвенными каналами утечки называют:_____
8. К косвенным каналам утечки информации относятся: ____
9. Непосредственными каналами утечки называют: _____
10. К непосредственным каналам утески информации относятся:

11. Избирательная политика безопасности подразумевает, что:
12. Полномочная политика безопасности подразумевает, что:
13. Достоверная вычислительная база - это:_____
14. Достоверная вычислительная база выполняет задачи: _____
15. Уязвимость информации — это: _____
16. Идентификация объекта - это: _____
17. Параллельная схема идентификации позволяет увеличить:
18. Какие существуют формы представления объектов, аутентифицирующих пользователя:
19. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:
20. Внешние объекты могут быть технически реализованы на различных носителях информации?
21. Для чего были разработаны протоколы идентификации с нулевой передачей знаний:
22. Механизм запроса-ответа используется для: _____
23. Кто разработал алгоритм идентификации с нулевой передачей знания:
24. Схему идентификации с нулевой передачей знаний предложили:
25. Для чего создается система разграничения доступа к информации:
26. Сбои, отказы технических и программных средств могут быть использованы для НСД?
27. Правильность функционирования ядра безопасности доказывается путем:
28. Мандатное управление позволяет упростить процесс регулирования доступа?
29. Матричное управление доступом предполагает использование:
30. Основной проблемой создания высокоэффективной защиты от НСД является:
31. Аппаратно-программные средства криптографической защиты информации выполняют функции:
32. Надежность защиты информации в компьютерной системе определяется:
33. Использование аппаратных средств снимает проблему:_____
34. Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются
35. К частично контролируемым компьютерным системам можно отнести современные КС, использующие:
36. Безопасность в частично контролируемым компьютерных системах может быть обеспечена:
37. К основным компонентам сети относятся: _____
38. В качестве ключевых носителей устройств криптографической защиты
39. данных серии КРИПТОН используются: _____
40. Средства серии КРИПТОН независимо от операционной среды
41. обеспечивают: _____

42. В системе Secret Disk используется: _____
43. В чем заключается особенность системы Secret Disk:_____
44. Мастер-ключ в Устройствах криптографической защиты данных серии
45. КРИПТОН загружается: _____
46. Криптографических функций в устройствах криптографической защиты
47. данных серии КРИПТОН выполняются: _____
48. Абонентские места, персональные компьютеры или терминалы клиента являются основными компонентами сети?
49. Возможные каналы утечки информации по классификации разделяют:
50. К группе каналов утечки информации в которой основным средством
51. является человек, относятся следующие утечки:_____
52. К группе каналов утечки информации в которой основным средством
53. является аппаратура, относятся следующие утечки: _____
54. К группе каналов утечки информации в которой основным средством
55. является программа, относятся следующие утечки: _____
56. К средствам активной защиты относятся: _____
57. К средствам пассивной защиты относятся: _____
58. К средствам собственной защиты относятся:_____
59. Может ли информативный сигнал в сети электропитания быть каналом утечки информации?
60. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:
61. Технические мероприятия направлены: _____
62. Организационными мероприятиями предусматривается:_____
63. Активные способы защиты информации при ее утечке через сеть
64. электропитания направленные на:_____
65. Пассивные способы защиты информации при ее утечке через сеть
66. электропитания направленные на:_____
67. Для минимизации паразитных связей внутри ПЭВМ используются:
68. Под системой защиты от несанкционированного использования и
69. копирования понимается
70. Под надежностью системы защиты от несанкционированного
71. копирования понимается:
72. Методы, затрудняющие считывание скопированной информации
73. основываются на: _
74. Для защиты от несанкционированного использования программ могут применяться электронные ключи?
75. Мероприятия по инженерно-технической защите информации от утечки
76. по электромагнитному каналу подразделяются на: _____
77. Любая криптографическая система основана на использовании:
78. В симметричной криптосистеме отправитель и получатель сообщения
79. используют: _

80. Асимметричная криптосистема предполагает использование:
81. Под ключевой информацией понимают: _____
82. В каких режимах может выполняться изучение логики работы

Критерии оценки:

- оценка «отлично» выставляется студенту, если полностью владеет как теоретическими знаниями, так и практическими навыками, отвечает на поставленные вопросы
- оценка «хорошо» - владеет теоретическими знаниями, обладает практическими навыками, затрудняется ответить на поставленные вопросы
- оценка «удовлетворительно» владеет только основами теоретического аспекта разбираемой темы
- оценка «неудовлетворительно» не обладает ни теоретическими знаниями, ни практическими навыками, не отвечает на контрольные вопросы

Перечень вопросов к экзамену (7 семестр).

1. Основные функции подсистемы защиты ОС.
2. Базовая политика безопасности.
3. Специализированные политики безопасности.
4. Избирательная и полномочная политика безопасности.
5. Процедуры безопасности.
6. Разработка политики безопасной организации.
7. Управление информационными потоками.
8. Достоверная вычислительная база.
9. Механизмы защиты ДВБ.
10. Принципы реализации политики безопасности.
11. Основные критерии оценки безопасности систем.
12. Роли и ответственность в безопасности сети.
13. Идентификация и аутентификация пользователя.
14. Аутентификация на основе многоразовых паролей.
15. Аутентификация на основе одноразовых паролей.
16. Строгая аутентификация. Основные понятия.
17. Типовые схемы идентификации и аутентификации пользователя.
18. Взаимная проверка подлинности пользователей.
19. Упрощенная схема идентификации с нулевой передачей знаний.
20. Параллельная схема идентификации с нулевой передачей знаний.
21. Схема идентификации Гиллоу-Куискуотера.
22. Защита информации в КС от несанкционированного доступа.
23. Управление доступом (Система разграничения доступа к информации в КС).
24. Состав системы разграничения доступа (Система разграничения доступа к информации в КС).

25. Концепция построения систем разграничения доступа.
26. Организация доступа к ресурсам КС.
27. Обеспечение целостности и доступности информации в КС.
28. Основные понятия криптографической защиты информации.
29. Симметричные криптосистемы шифрования.
30. Асимметричные криптосистемы шифрования.
31. Функции хеширования.
32. Электронная цифровая подпись.
33. Управление криптоключами.
34. Корпоративная информационная системы.
35. Архитектура «облачных сервисов».
36. Подсистемы информационной безопасности традиционных КИС.
37. Средства защиты в виртуальных средах.
38. Обеспечение безопасности «облачных» сред на базе пакета Trend Micro Deep Security.
39. Защита на канальном уровне. Протокол PPTP.
40. Защита на канальном уровне. Протокол L2TP.
41. Защита на сетевом уровне. Архитектура средств безопасности IPSec.
42. Защита передаваемых данных с помощью протоколов AH и ESP.
43. Протокол управления криптоключами IKE.
44. База данных SAD и SPD.
45. Особенности реализации средств IPSec и их преимущества.
46. Протоколы SSL и TLS.
47. Протокол SOCKS.
48. Особенности безопасности беспроводных сетей.
49. Функции межсетевых экранов.
50. Фильтрация трафика (технологии межсетевого экранирования).
51. Выполнение функций посредничества.
52. Межсетевые экраны.
53. Классификация сети VPN и Средства обеспечения безопасности VPN.
54. Функционирование системы управления доступом.
55. Аутентификации удаленных пользователей на основе одноразовых паролей OTP.
56. Протоколы аутентификации удаленных пользователей. Протокол PAP.
57. Протоколы аутентификации удаленных пользователей. Протокол CHAP.
58. Протоколы аутентификации удаленных пользователей. Протокол EAP.
59. Протоколы аутентификации удаленных пользователей. Протокол S/Key.
60. Протоколы аутентификации удаленных пользователей. Протокол

Kerberos.

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Фонд оценочных средств дисциплины включает в себя контрольные вопросы, задания контрольных работ, вопросы для промежуточной аттестации.

Виды самостоятельной работы обучающихся

Изучение основной и дополнительной литературы по материалам курса.

Выполнение заданий самостоятельной работы по курсу.

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
3	5	0	15	35	0	5	40	100

Программа оценивания учебной деятельности студента Семестр 7

Лекции. Посещаемость, опрос, активность за семестр — от 0 до 5 баллов. **Лабораторные занятия. Выполнение одной лабораторной работы – 10б.**

Практические занятия. Посещаемость, опрос, активность за семестр — от 0 до 15 баллов.

Самостоятельная работа.

Контроль выполнения заданий самостоятельной работы в течение одного семестра — от 0 до 25 баллов;

Контрольная работа (от 0 до 10 баллов);

Таким образом, студент в течении 3-го семестра может получить от 0 до 35 баллов.

Автоматизированное тестирование. **Не предусмотрено.**

Другие виды учебной деятельности.

Написание реферата является одной из форм обучения студентов. Данная форма обучения направлена на организацию и повышение уровня самостоятельной работы студентов. Реферат, как форма обучения студентов - это краткий обзор максимального количества доступных публикаций по

заданной теме, подготовка самого реферативного обзора и презентации по нему. При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируется уже сделанные выводы и в связи с небольшим объемом данной формы работы. Преподавателю предоставляется сам реферат в письменной форме (электронная версия в формате Microsoft Word) и презентация к нему (электронная версия в формате PowerPoint). Сдача реферата происходит в форме защитыдоклада с использованием подготовленной презентации.

Критерии оценки рефератов:

Оценки на "отлично":

10 - тема раскрыта блестяще, презентация является целостным новым независимым дополнением высокого уровня к лекционному курсу

9 - тема раскрыта отлично, есть отдельные фрагменты, которые являются новыми независимыми смысловыми дополнениями к лекциям

8 - тема в основном раскрыта, качество материала высокое, но не является уникальным

Оценки на "хорошо"

7 - тема раскрыта не полностью, не хватает некоторой части. Качество материала хорошее.

6 - тема раскрыта не полностью, не хватает некоторой значимой части.

Удовлетворительно:

5 - раскрыта хотя бы примерно половина темы. Качество материала удовлетворительное.

4 - что-то по существу реферата сказано, но мало и фрагментарно. Качество материала на грани удовлетворительного.

Неудовлетворительно:

3 - понял, о чем надо рассказывать, но практически ничего не рассказал по теме реферата. Качество материала неудовлетворительное.

2 - понял название темы, ничего не рассказал либо рассказывал не о том. Материал фактически отсутствует.

1 - не понял название темы, не рассказывал. Материал фактически отсутствует и не по теме.

0 - реферат не сдавался.

Промежуточная аттестация. Методика оценивания знаний обучающихся по дисциплине «Облачные технологии» в ходе промежуточной аттестации:

25-40 баллов:

Ответ студента содержит:

глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;

знание концептуально-понятийного аппарата всего курса;

знание монографической литературы по курсу,

также свидетельствует о способности:

самостоятельно критически оценивать основные положения курса;

увязывать теорию с практикой.

15-24 баллов:

Ответ студента свидетельствует:

о полном знании материала по программе;

о знании рекомендованной литературы,

а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

1-14 баллов:

Ответ студента содержит:

поверхностные знания важнейших разделов программы и содержания лекционного курса;

затруднения с использованием научно-понятийного аппарата и терминологии курса;

стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала ставится оценка 0 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за один семестр по дисциплине «Облачные технологии» составляет 100 баллов.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **Экзамен**. Экзамен проводится в форме тестирования. При соответствии ответа учащегося на зачете более чем 51 % критериев из этого списка выставляется оценка «удовлетворительно», 66% – 85% оценка «хорошо», 86% и выше оценка «отлично».

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. **Правовое обеспечение информационной безопасности** : [учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность", 075500 "Комплекс. обеспечение информ. безопасности и автоматизир. систем", 075600 "Информ. безопасность телекоммуникац. систем" / С.Я.Казанцев и др.]; под ред. С.Я.Казанцева. - М. : Academia, 2005. - 239 с. : ил. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 235-237. - Допущено УМО. - ISBN 5-7695-1209-1 : 129-47

2. **Филин С. А.** Информационная безопасность : учеб. пособие / Филин, Сергей Александрович. - М. : Альфа-Пресс, 2006. - 411 с. - ISBN 5-94280-163-0 : 129-03.

3. **Галатенко В. А.** Стандарты информационной безопасности : курс лекций: учеб. пособие / Галатенко, Владимир Антонович ; под ред. В.Б.Бетелина; Интернет-ун-т информ. технологий. - 2-е изд. - М. : ИНТУИТ.ру, 2006. - 263 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 : 176-00.

4. **Уколов В. Ф.** Теория управления : учеб. для вузов / Уколов, Владимир Фёдорович, А. М. Масс, И. К. Быстряков. - 3-е изд., доп. - М. : Экономика, 2007. - 696 с. - Допущено МО РФ. - ISBN 978-5-282-02698-6 : 260-00

5. **Галатенко В. А.** Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.

6. Петров С. В. Информационная безопасность : учеб. пособие /. - Новосибирск: М. : АРТА, 2012. - 439-77.

б)дополнительная:

1. ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements.Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы./ http://www.27000.org/

2. Аудит информационной безопасности. Под ред. А.П.Курило. - М: БДЦ-Пресс, 2014.

3. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005)./ http://www.27000.org/

4. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью./ http://www.27000.org/Международный стандарт. ISO/IEC 27003:2005

Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью./ http://www.27000.org/

5. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью./ http://www.27000.org/

6. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности./ http://www.27000.org/

7. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью./ http://www.27000.org/

8. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью./ http://www.27000.org/

9. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2012.

10. Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: ДМК пресс, 2013.

14

11. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Стандарты и качество, 2014.

12. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. - М.: Академия, 2008 г. - 192 стр.

13. Золотарев Управление информационной безопасностью. Ч. 1. Анализ информационных рисков - Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. ЭБС IPRbooks: http://www.iprbookshop/ru/
2. Электронно-библиотечная система «Университетская библиотека онлайн»(архив):www.dub.m
3. Единое окно доступа к образовательным ресурсам. http://window.edu.ru/
4. http://www.microsoft.com/msf
5. http://www.uml.org
6. http://www.wikipedia.org

10. Методические указания для обучающихся по освоению дисциплины. ***Критерии и показатели сформированности компетенций***

Степень (уровень) сформированности компетенций на этапе изучения дисциплины «Основы управления информационной безопасностью» оценивается по следующим критериям: мотивационно-ценностный,

когнитивный, операционно-деятельностный. Показателями критериев являются результаты обучения по дисциплине (дескрипторы) таблицы 1. Инструментарий, этапы измерения показателей и критериев компетенции представлены в таблице.

Критерии сформированности компетенции	Способы оценки	
	Этапы контроля	Средства оценки
Мотивационно-ценностный критерий	4, 6, 7, экзамен	1
Когнитивный критерий	4, 5, 6, 7	1
Операционно-деятельностный критерий	4, 5, 7	1
	6, экзамен	
Интегральная оценка	Экзамен	1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Этапы контроля: раздел 2 (самостоятельная работа), раздел 3 (самостоятельная работа), раздел 4

(самостоятельная работа), раздел 5 (самостоятельная работа), раздел 6 (самостоятельная работа),

раздел 7 (самостоятельная работа), экзамен.

Время на выполнение: 60 мин.

Метод оценивания: автоматизированный

Критерии оценки результатов выполнения: менее 50% правильных ответов - неудовлетворительно, менее 65% - удовлетворительно, менее 86% хорошо, 86% и более - отлично.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и

информационных справочных систем.

Информационные технологии Образовательный процесс осуществляется с применением локальных и распределенных информационных технологий (таблица 4, 5).

Таблица 4 - Локальные информационные технологии

Группа программных средств	Наименование программного продукта
Офисные программы	Microsoft Office
	Libre Office

Средства разработки	MicroSoft Visual Studio 2015 MicroSoft SQL Server 2012 VipNet Client 4 Dallas Lock 8.0 КриптоПро CSP

Таблица 5 - Распределенные информационные технологии

Группа	Наименование
Система тестирования	Система сетевого компьютерного тестирования ДГУ www.ts.icc.dgu.ru
Библиотеки и образовательные ресурсы	Электронная библиотека ДГУ http://www.elib.dgu.ru
	Кафедральные сайты ДГУ http://cafedra.dgu.ru
	Сайте электронных образовательных ресурсов ДГУ http://eor.dgu.ru
Система электронного обучения	Сервер электронного обучения moodle http://moodle.dgu.ru

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Таблица 6 - Материально-техническая база

Помещения для осуществления образовательного процесса	Перечень основного оборудования (с указанием кол-ва посадочных мест)	Адрес (местоположение)
Аудитории для проведения лекционных занятий		
Лекционные аудитории	Интерактивная доска, ноутбук; проектор. Количество посадочных мест - 30.	Ауд. 3-14, 4-16, 2-10, учебный корпус № 8, г.Махачкала, ул. Джержинского, 12.
Аудитории для проведения лабораторных занятий, контроля успеваемости		

Компьютерный класс	Компьютеры с выходом в Интернет и доступом в электронную информационно- образовательную среду вуза. Количество посадочных мест - 15.	Компьютерный зал № 2 учебный корпус № 3, г.Махачкала, ул. Джержинского, 12.
Помещения для самостоятельной работы		
Компьютерные классы	Компьютеры с выходом в Интернет и доступом в электронную информационно-	Компьютерный зал № 1, учебный
	образовательную среду вуза. Количество посадочных мест - 15	корпус № 3, г. Махачкала, ул. Джержинского, 12.
Читальный зал библиотеки ДГУ	Компьютеры с выходом в Интернет и доступом в электронную информационно- образовательную среду вуза. Количество посадочных мест - 30.	Электронный читальный зал научной библиотеки ДГУ, г. Махачкала, ул. Батырая, 4